SOA paper crunch

Data security and encryption in low-power wireless sensor networks

Ioan Deaconu AAC

Andrei Mușat AAC

Advanced Operating Systems

26 Novemver 2014

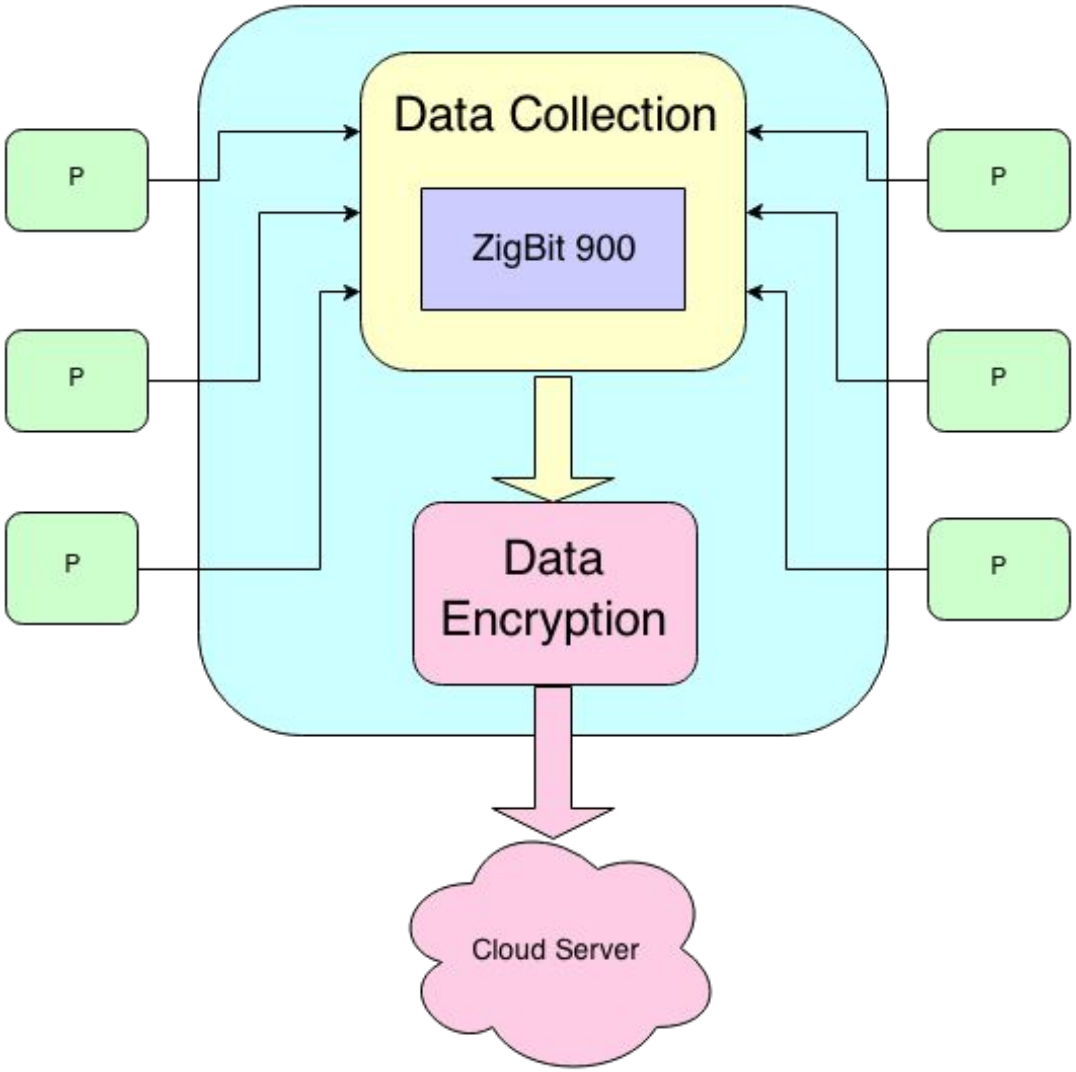
Context

- Sensor nodes equipped with peripherals for environment monitoring
- Grouped into a Wireless Sensor Network
- Main function is to monitor vibrations in order to predict earthquakes
- Data transmitted is important and sensitive

Related Work

- Classification by Vartika Shah, Sanjiv Sharma
- SPIN protocol – CTR encryption with master key. Protects against data and information spoofing and message replay attacks.
- TinySec/TinyOs – CBC encryption with symmetric key. Protects against data and information spoofing and message replay attacks.
- LEAP – RC5 encryption using various key types: individual, group, cluster, etc. Protection against flood attacks, spoofing, selective forwarding etc.

Node Architecture Diagram



Progress

- Attempt two directions: one using hardware resources (AES), the other software implementations
- Hardware direction: use AES supported ECB encryption/decryption for inter-node communication and CBC encryption for data
- Software direction: implementing Skipjack and RC5 algorithms to use for benchmarking

Expected Results

- Protection against data replication and spoofing
- Protection against “man in the middle” attack types
- Encryption algorithm must be fast and capable of handling high amounts of data
- Power consumption should be kept as low as possible

Problems Encountered

- Atmega1281 microcontroller does not support hardware encryption. AES is implemented in the wireless transceiver instead.
- Time spent encrypting data contends with time spent sampling the peripherals
- Transmissions are less frequent
- Time spent processing and encrypting data is proportional with power consumption, hence reduces node autonomy